

# Colombia

# 66

/100

PARTLY FREE

|                                     |        |
|-------------------------------------|--------|
| A. <u>Obstacles to Access</u>       | 18 /25 |
| B. <u>Limits on Content</u>         | 26 /35 |
| C. <u>Violations of User Rights</u> | 22 /40 |

## LAST YEAR'S SCORE &amp; STATUS

67 /100    **Partly Free**

Scores are based on a scale of 0 (least free) to 100 (most free)

[TOP](#)

## Overview

Internet access continues to expand in Colombia, and government initiatives aiming to bridge the digital divide have been implemented during the coverage period. However, the online sphere remained constrained by excessive surveillance of individuals, including journalists, and coordinated progovernment social media posts. Concerns over the impact of disinformation and misinformation online were also raised as mass protests took place at the end of 2019.

Colombia is among the longest-standing democracies in Latin America, but one with a history of widespread violence and serious human rights abuses. Violence related to the conflict has declined in recent years, and public institutions have demonstrated the capacity to check executive power and enforce the rule of law. The government and the country's main left-wing guerrilla group signed a peace accord in 2016, but Colombia still faces enormous challenges in consolidating peace and guaranteeing political rights and civil liberties throughout its territory. Human rights defenders are the targets of lethal attacks.

## **Key Developments, June 1, 2019 - May 31, 2020**

- Several initiatives aiming to close the country's digital divide were implemented, including the ongoing deployment of free, 24-hour access points and the March 2020 introduction of subsidized internet fees (see A2).
- In May 2020, the Supreme Court ruled in favor of a law that significantly impacted the information and communication technology (ICT) regulatory environment by placing numerous responsibilities into a restructured public commission, superseding an existing public body (see A5).
- A December 2019 Supreme Court decision found blog and online forum operators liable for defamatory user comments, and news outlets faced pressure to remove content from their sites. In March 2020, journalist Edison Lucio Torres served a 10-day prison sentence after he refused to remove articles from his news site and personal website (see B2 and C3).
- In September 2019, a WhatsApp group comprised of President Iván Duque's allies, including administration officials, was formed to coordinate progovernment social media activity and attack critics. During protests held

**TOP**

later in the year, Democratic Center (CD) party members tried to distort the narrative on social media (see B5 and B8).

- January and May 2020 articles from magazine *Semana* revealed that the military used open-source and more sophisticated technology to engage in surveillance, and specifically targeted at least 130 people, including politicians, magistrates, generals, and journalists (see C5).
- In March 2020, the government authorized mobile service providers to share user data with public authorities responding to the COVID-19 pandemic; the circular that triggered this activity did not provide a clear time limit on data collection, nor did it specify what should be collected (see C6).

## A. Obstacles to Access

*While obstacles to internet access remain in Colombia, several initiatives aiming to bridge the digital divide were implemented during the coverage period. A new ICT law, which was passed in 2019 and was upheld in a May 2020 Supreme Court ruling, was criticized for lacking safeguards to protect the independence of a new, powerful regulator.*

**A1** 0-6 pts

**Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?**

**4/6**

Internet access continues to increase in Colombia. According to official figures, fixed internet connections increased from 13.45 for every 100 inhabitants at the end of 2018 to 13.81 at the end of 2019, while mobile connectivity increased from 27.4 million to 30.9 million connections during the same period. <sup>1</sup> However, the rate of growth in fixed-access services decreased, from 4.7 percent between 2017 and 2018 to 2.6 percent between 2018 and 2019. <sup>2</sup>

Obstacles to access remain, including a lack of infrastructure in rural areas, low levels of digital literacy, and high prices for service (see A2). The government has worked to address the lack of connectivity in the country, especially in remote and isolated areas. In January 2020, the ICT minister announced a plan aimed at connecting 20 million residents to broadband services. <sup>3</sup>

**TOP**

Colombia ranks relatively low in global rankings of mobile and fixed broadband speeds. Speedtest recorded an average fixed download speed of 28.29 Mbps and an average mobile download speed of 18.67 Mbps in April 2020, <sup>4</sup> compared to global averages of 74.74 Mbps and 30.89 Mbps, respectively. Colombia's Commission for Communications Regulation (CRC) updated the speed standards for broadband for 2019, stating that minimum download speeds of 25 Mbps and upload speeds of 5 Mbps are needed in order to be considered broadband. <sup>5</sup>

In 2018, the then incoming government of President Duque launched a new policy for the sector called "El futuro digital es de todos" (the digital future belongs to everyone), with an emphasis on public- and private-sector cooperation. <sup>6</sup> In February 2020, the results of a December 2019 spectrum auction, that is expected to connect 3,658 remote and rural areas between 2020 and 2025, was formalized. Blocks of radio spectrum were awarded to providers Claro, Tigo, and Novator Partners, <sup>7</sup> but Novator Partners declined one of the blocks in January 2020, leading to a legal dispute. <sup>8</sup> In late February 2020, the government announced that Novator Partners would have to pay 42 billion Colombian pesos (\$11.2 million) <sup>9</sup> to the state for declining the spectrum block. <sup>10</sup>

## A2 0-3 pts

**Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?**

**2/3**

*Score Change: The score improved from 1 to 2 due to initiatives implemented during the coverage period that aim to bridge the digital divide, including the introduction of subsidized internet fees and the creation of Rural Digital Zones.*

Geographic and socioeconomic disparities in internet access are significant, but efforts to address them have been introduced. According to the Colombian Chamber of Information Technology and Telecommunications (CCIT), an ICT trade association, 75 percent of higher-income people have internet access, compared to fewer than 50 percent of lower-income people. There is also a gap between urban and rural areas; over 80 percent of people are disconnected in some regions. <sup>11</sup> The National University of Colombia's (UNAL) *Great ICT Survey 2019* found that 40 percent of

**TOP**

residents lacked fixed-broadband access, and only 26 percent of rural households had a connection. <sup>12</sup>

While Colombia continues to face divides in access and challenges in reducing them, the coverage period saw notable efforts to address these gaps. In March 2020, the ICT ministry announced subsidized monthly internet fees ranging from 8,613 pesos (\$2.30) to 19,074 pesos (\$5.10) for users in isolated and rural areas. The ministry, which also presides over the Last Mile Program that aims to provide access to 500,000 low-income households, additionally reported that nearly 270,000 subsidized fixed connections had already begun to be installed. <sup>13</sup>

The ICT ministry engaged in other initiatives to improve rural access before and during the coverage period. The first phase of the Universal Sustainable Access Project's draft plan was released in March 2019, <sup>14</sup> and aims to benefit 1,000 population centers in 378 municipalities in 20 of Colombia's departments. Internet access is provided through Digital Zones, which allow anyone to access the internet without charge, 24 hours a day, from smartphones, tablets, or laptop computers. Between October and November 2019, a total of 1,000 Rural Digital Zones were installed, and are scheduled to operate through the second half of 2021. Meanwhile, the National Project of Universal Access for Rural Areas aims to connect 10,000 remote and rural population centers in 32 departments between November 2020 and the project's scheduled June 2022 completion. <sup>15</sup>

In recent years, Colombia has ranked highly in the Affordability Drivers Index (ADI) report, which measures policy and regulatory factors that can enable more affordable broadband. The latest report ranked Colombia in second place, citing sound regulatory decisions to improve affordability and access in the country. <sup>16</sup>

During the COVID-19 pandemic, internet service providers (ISPs) focused on maintaining robust internet access as users worked from home, and offered higher data and speeds to subscribers free of charge. <sup>17</sup>

**A3** 0-6 pts

**Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?**

**TOP**

**6/6**



The government does not place limits on bandwidth, nor does it impose control over infrastructure, except in emergency situations when ISPs are required to make their infrastructure available for official responses. <sup>18</sup> The government has not centralized telecommunications infrastructure and does not deliberately shut down internet or mobile connections.

Colombia has only one internet exchange point (IXP), NAP Colombia, through which ISPs exchange traffic to improve efficiency and speed. Located in Bogotá, the IXP is managed by the Colombian Chamber for Informatics and Telecommunications (CCIT).

<sup>19</sup>

**A4** 0-6 pts

**Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?**

**4/6**

Colombia is home to more than 300 ISPs. <sup>20</sup> While approximately 75 percent of the market is concentrated in the hands of three companies, there are nonetheless multiple options for consumers and healthy competition. <sup>21</sup> The market is led by three providers: Claro, with a 38-percent user share, followed by UNE with 22 percent, and Movistar with 14.2 percent. <sup>22</sup> Nonetheless, market entry is straightforward, and it is possible for anyone to establish an ISP by following the general requirements of the ICT Law, which establishes free competition and prioritizes efficient use of infrastructure and access to ICTs. <sup>23</sup> The fixed internet market registered, in the fourth quarter of 2019, 335 providers with at least one active connection. 316 of these had less than 10,000 clients. <sup>24</sup>

Registration requirements are neither excessive nor onerous. Business owners must provide personal and tax identification as well as a description of services, but no fee is required. This information is published in an open registry, and the ICT ministry has 10 days to verify the data before the business may begin operating. Registration can be denied when information is incomplete or false, or when an ISP does not have the proper commercial status to offer the necessary services. <sup>25</sup> ISPs must also apply for licenses to utilize the radioelectric spectrum, although there have been no complaints of difficulties or bias with this process.

**TOP**

The mobile landscape is more concentrated. Although there are nine providers, nearly 93 percent of the market is in the hands of three companies: Claro (54.7 percent), Movistar (23.3 percent), and Tigo (14.3 percent). <sup>26</sup> Mobile service providers must contribute 0.01 percent of their annual income to an ICT ministry fund, Fontic, which is devoted to the development of nationwide ICT projects.

The ICT modernization law, which was passed by Congress in June 2019 (see A5) and aims to increase connectivity, risks maintaining and augmenting market concentration by favoring more established and larger telecommunications providers. The spectrum licensing period, for instance, was extended from 10 years to up to 20. <sup>27</sup> While this extension provides more stability for private investments, it could limit competition at the infrastructural level. The law has also been criticized for helping to foster competition between community networks and major providers.

In addition, while service providers were previously obligated to pay a contribution of 0.01 percent of their annual income to Fontic, the amount provided to a new public fund will vary depending on ambiguous qualitative variables such as “social benefit.” Moreover, these criteria will be determined at the ICT minister’s discretion. A share of the fund will be used to increase connectivity, and service providers that partner with the government to do so will be allowed to pay up to 60 percent of their contribution in kind, also at the ICT minister’s discretion. <sup>28</sup>

**A5** 0-4 pts

|                                                                                                                                                     |              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <b>Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?</b> | <b>2 / 4</b> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------|

The regulation of Colombia’s ICT sector changed significantly during the coverage period. In June 2019, Congress approved a new law for the sector after months of contentious debate. It notably eliminates the National Television Authority (ANT) and establishes a convergent regulator—through a restructured Communication Regulation Commission (CRC)—to regulate the ICT sector, television, and rad Critics of the law contended that the new regulatory body concentrates too many functions in the government, and lacks independence. <sup>29</sup> In a move criticized by the Organization for Economic Co-operation and Development (OECD), the law also establishes two decision-making entities within the CRC: the Commission for Audiovisual Content (CCA), covering issues related to pluralism and audiences, and

the Communications Commission (CC), dealing with technical and market regulation. The CCA has three members, two chosen through a public contest and one chosen by regional channels. The CC has five: the ICT minister, a commissioner chosen by the president, and three selected by the government through an open application process. <sup>30</sup> In May 2020, the Constitutional Court rejected a legal challenge to the new law. <sup>31</sup>

The president appoints the ICT minister, who oversees the telecommunications sector through the ministry; that minister is also responsible for leading the CRC. <sup>32</sup> The minister also designates the head of the National Spectrum Agency (NSA), which manages Colombia's radioelectric spectrum. Some have suggested that this executive-driven design prevents objective oversight of the sector and affords the president undue influence over its operations.

The selection process for the current CC members, who assumed their posts in February 2020, <sup>33</sup> raised questions about the process's independence. Applicant Sergio Martínez took first place in the open call for candidates, followed by Paola Bonilla. Martínez initially declined the role but President Duque subsequently appointed him to the CC, leaving Bonilla to become a commissioner as well. <sup>34</sup>

Since 2010, a government-appointed concessionaire has been responsible for allocating the .co domain. For the domains org.co, edu.co, mil.co, and gov.co, applicants must comply with specific requirements; for edu.co, for example, the applicant must be an educational institution. <sup>35</sup> During the coverage period, the process for awarding a public tender for the administration of the .co domain was mired in public and legal controversy; the selection, managed by the ICT ministry, was criticized for irregularities in calculating qualified bidders, leading the attorney general's office to request a suspension to the tender process. ICT minister Sylvia Constaín resigned in May 2020, reportedly due to the flawed process. That same month, the tender was awarded to .CO Internet SAS, which was previously suspected of managing the .co domain. <sup>36</sup>

## B. Limits on Content

TOP

*Blocking or filtering of political, religious, or social content is not common in Colombia, but a December 2019 Supreme Court decision held blog and forum*



operators liable for defamatory user comments, while news outlets were pressured to remove content from their sites. An investigation during the coverage period revealed that government supporters coordinated through a WhatsApp group to author progovernment content and attack critics. During mass protests, organized in part online, supporters and politicians from Duque's party, the CD, tried to distort the narrative on social media.

**B1** 0-6 pts

**Does the state block or filter, or compel service providers to block or filter, internet content?**

**5/6**

Blocking or filtering of political, religious, or social content is not a regular occurrence in Colombia. **37** YouTube, Facebook, Twitter, and international blog-hosting services are freely available.

While no content is systematically blocked under Colombian law besides child sexual abuse images, in September 2018, Colombia's gambling regulator submitted a list of over 1,800 gambling sites to be blocked by ISPs, following the approval of online gambling legislation in 2016, that requires gambling sites to apply for a license. The regulator found that the sites were operating without authorization. **38** As of March 2020, 3,365 such websites were reportedly ordered to be blocked. **39**

Apps that rely on the internet to provide commercial services, such as Uber, have been the center of much debate, and the government has been trying to regulate Uber with little success. While the transportation ministry has argued in favor of blocking the app, **40** the ICT ministry has invoked the net neutrality principle, which does not allow network operators to discriminate against specific content or services. ICT officials said that there are no grounds for blocking Uber, which is not illegal. **41**

**B2** 0-4 pts

**Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?**

**2/4**  
**TOP**

*Score Change: The score declined from 3 to 2 due to a December 2019 Supreme Court decision that makes blog and forum operators more likely to remove user-*

*authored content, and because news outlets have additionally been pressured to remove content.*

The Colombian government does not regularly order the removal of content, though a problematic Supreme Court ruling could facilitate future restrictions. Periodic court cases have resulted in judicial orders requiring the removal of specific information deemed to violate fundamental rights. News outlets separately report receiving threats intended to force them to remove content, as well as requests to eliminate content based on the “right to be forgotten.” <sup>42</sup>

In December 2019, the Supreme Court ruled that blog and forum operators would be legally responsible for third-party defamatory user comments if they did not adopt mechanisms to control them. The decision was criticized for creating an incentive to excessively restrict comments or totally eliminate comment sections. <sup>43</sup>

Separately, a site that publishes consumer complaints against a government entity was repeatedly accused of infringing on that entity’s trademark, resulting in its removal. The website icetextearruina.com was first taken down in March 2016 by hosting provider GoDaddy on the basis of a complaint from ICETEX, an official entity in charge of student loans. The website is owned by the Association of Users of Student Loans (ACUPE), a legally recognized organization that denounces allegations of abuse involving loans. Civil society organizations said ICETEX was abusing GoDaddy’s complaints system to censor the allegations. <sup>44</sup> The site remained inaccessible during the coverage period of this report. <sup>45</sup> In March 2020, ICETEX’s Facebook page was closed by the platform, <sup>46</sup> but was reinstated after the incident was shared with Facebook representatives in Colombia. <sup>47</sup>

**B3** 0-4 pts

**Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?**

**3/4**

Colombian authorities and courts place some restrictions on digital content, <sup>with</sup> some of these decisions taking place in an opaque environment and with sparse or no public explanation; this is especially true in cases of images depicting sexual abuse against children and online gambling. Users have limited avenues to appeal blockings or restrictions. <sup>TOP</sup>

Police and other institutions may limit content on a range of topics, from sexual abuse to “inappropriate content” or “other issues,” in order to protect minors. <sup>48</sup> Child sexual abuse images, which are illegal under international law, are subject to blocking.

<sup>49</sup> Decree 1524 (2002) requires ISPs to undertake technical measures to prevent the online availability of child sexual abuse images. <sup>50</sup> The possibility for civil or judicial oversight for restriction of such content is limited because information about which websites are blocked is classified—possibly out of fear that individuals would use circumvention tools to access such material if a list of banned sites were made public.

<sup>51</sup> The multistakeholder group Te Protejo (I Protect You) is an alliance led by the civil society organization RedPaPaz, and reports websites that host child sexual abuse images to the authorities. <sup>52</sup>

Online gambling legislation also allows for the blocking of websites, but there is no centralized, public reporting system for why sites are blocked, and the reason is not always disclosed. Users are sometimes redirected to pages displaying the reason a website is blocked, but this does not always occur. In some cases, entire websites are blocked due to the nature of advertisements. <sup>53</sup>

In 2017, the ISP ETB began to publish a transparency report on blocking orders, followed by four other ISPs in 2018. Nevertheless, the information that is given is not always comprehensive. Fundación Karisma, in their December 2018 report *Dónde están mis datos* (Where is my data), notes that while information on the blocking of child sexual abuse images is somewhat clear, blockings related to gambling and cases of emergency are more opaque. In addition, there are no mechanisms to appeal blocking decisions. <sup>54</sup>

In September 2019, Colombia’s Constitutional Court ruled on a case partially originating from a customer’s blogger.com entry that accused a furniture warehouse of engaging in scams. In 2017, a lower court held that blogger.com’s owner, Google, had to remove the post and monitor the platform, but that ruling was overturned in 2018 over its potential constitutional relevance. The Constitutional Court’s decision included guidelines on removing online content in an effort to balance freedom of expression with the violation of one’s good name. <sup>55</sup>

**TOP**

Several months earlier, in April 2019, the Constitutional Court held that the right to freedom of expression was violated when Jael Johana Castro León was pressured to remove a Facebook post. The post, which claimed that Santander University Hospital

official Sigifredo Fonseca González was part of a corrupt cartel, was allegedly defamatory, leading him to sue Castro León for insulting his name, honor, and privacy.

**56**

In 2015, a court ruling strengthened the precedent that search engines should not be held liable for linking to content, even if the content has been found to violate the law.

**57** Although observers praised the fact that it exempted intermediaries from liability,

**58** some worried that the ruling might place an excessive burden on other digital content producers or publishers, because it required an online newspaper involved in the case to take steps to make the disputed information in question harder to find. **59**

**B4** 0-4 pts

**Do online journalists, commentators, and ordinary users practice self-censorship?**

**3/4**

Self-censorship is a notable problem for journalists and likely affects online publications. **60** According to the most recent national survey of journalists by Proyecto Antonio Nariño (PAN), an alliance of organizations focused on freedom of expression and access to information, 25 percent of respondents stated that they avoided publishing information due to fear of aggression; 21 percent feared losing their jobs or having their media outlets closed; and 21 percent knew about media that avoided publishing information due to fear of losing advertising revenue. **61**

According to a March 2019 report from Deutsche Welle (DW) Akademie, many private media outlets are owned by members of the country's elite, and members of press engage in self-censorship. The report also noted that many private media outlets rely heavily on advertising from large corporations and public agencies, and that newer outlets lack financial independence. While there is no indication that the owners of these newer outlets directly interfere in editorial decisions, their agendas may nevertheless influence coverage decisions. **62**

Nongovernmental organizations (NGOs) that focus on local press freedom have also reported a significant increase of online harassment against female journalists by politically-driven troll farms, which has led to some self-censorship. **63** Female activists also face online intimidation. **64**

**TOP**

**Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?**

**3/4**

Concerns about the manipulation of online information surfaced during the coverage period. In February 2020, journalistic coalition La Liga Contra El Silencio (The League Against Silence) published an investigation of a WhatsApp group that aimed to increase the social media impact of the CD and conducted organized attacks of government critics. According to the report, the group was created by diplomat Claudia Bustamante, and included Víctor Muñoz, then an advisor to President Duque. Other members included associates of former president Álvaro Uribe, members of the CD, and the founder of a news outlet that disseminated articles written by politicians. The WhatsApp group disbanded soon after its creation, but coordinated activity continued through at least the end of 2019; after its existence was revealed, Muñoz resigned from his post. <sup>65</sup>

During the COVID-19 crisis, the health ministry took steps to address misinformation, including by labelling content as “fake news.” <sup>66</sup> Misinformation also proliferated during widespread protests that took place in November 2019. According to a DFRLab report, xenophobic WhatsApp messages and tweets claimed that Venezuelans engaged in looting and vandalism. In addition, videos depicting one attempted looting were falsely attributed to multiple incidents in several cities. The videos were also featured by media outlets’ Twitter accounts, allowing the manipulated information to spread further. <sup>67</sup>

Concerns about the spread of disinformation and hateful content on social media networks surged during the hotly contested presidential campaign in 2018. In addition to Twitter and Facebook, WhatsApp was a popular platform for sharing misinformation: the project El Poder de Elegir (The Power to Choose) verified a number of such chains circulating on the closed messaging platform. <sup>68</sup>

**TOP**

In a study conducted between January and June 2018, the Electoral Observation Mission (MOE), an election monitoring group, found that “social media allowed a great conversation about the electoral process, but this was not necessarily more plural, transparent, or deliberative. The communities that share false information do



not interact with communities that deny it.” Moreover, it found that social networks generally performed a propagandistic function. **69**

In February 2018, a Twitter user found that a network of media portals that normally specialized in motorcycles, pets, maternity, and sports was being used to disseminate propaganda and misleading information favorable to then presidential candidate Duque. **70** That same month, a digital safety firm calculated how many fake followers the presidential candidates had on Twitter, and found that over 35 percent of the followers of the three most popular candidates on Twitter were fake. **71**

Concerns about the reach of online disinformation escalated ahead of run-off elections held in June 2018, as viral hoaxes made headlines. **72** That month, the attorney general’s office opened an investigation into the suspected author of false social media posts that urged voters to abstain in the second round, claiming that their first-round votes would still count. **73**

On the other hand, researchers did not find significant evidence of botnet operations. Looking at the amplifiers of misinformation, the Atlantic Council’s Digital Forensic Research Lab found that “the main vectors of false or misleading claims were not bots or ‘dark’ entities, but high-profile and well-known partisans or politicians.” **74**

**B6** 0-3 pts

**Are there economic or regulatory constraints that negatively affect users’ ability to publish content online?**

**2/3**

Many online news outlets are thought to avoid coverage of certain issues in order to maintain relationships with advertisers, whose purchases provide the outlets with revenue. According to the most recent national survey of journalists by PAN, between 40 and 66 percent of respondents believed that media outlets in their region modify their editorial positions to protect advertising revenue, depending on the region; 64 percent said that the way official advertising is awarded is opaque; and 75 percent agreed that it is necessary to change the way in which official advertising contracts are allocated. **75**

**TOP**

**B7** 0-4 pts

**Does the online information landscape lack diversity?**

Colombia has numerous digital media outlets and online spaces for political debate, and Colombians are able to view and disseminate a wide range of content.

Many professional media enterprises thrive in Colombia's largest cities and, in general, authorities do not interfere with their operations. However, there is a lack of media diversity in many regions. According to the Foundation for Press Freedom (FLIP), 19 of the 21 departments studied had no media presence to produce and disseminate local information. <sup>76</sup> Out of almost 1,335 media outlets operating in those regions, only 113 were digital, due to the low internet penetration rate outside large cities. <sup>77</sup>

During the COVID-19 crisis, local and national governments engaged in intensive public communications efforts. President Duque, for example, has made daily, hour-long television broadcasts that are also shared on social media, as well as numerous other media appearances. <sup>78</sup>

**B8** 0-6 pts

**Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?**

**5/6**

Large-scale antigovernment protests took place during the last two months of 2019, sparked by an announcement that benefits would be lowered for both workers and retirees. The social media hashtag #21N was employed to organize a national strike on November 21st. <sup>79</sup> The online discussion was highly polarized. After 18-year-old protester Dilan Cruz was killed by the police in an incident that sparked continued demonstrations, some CD politicians falsely accused him of vandalism, and Duque's supporters accused a left-wing politician of killing him by calling for protests. Antigovernment protesters, in contrast, used hashtags blaming the state for Cruz's death. <sup>80</sup>

The protests were otherwise largely peaceful, with some isolated episodes of <sup>TOP</sup>looting and vandalism, while security forces were accused of multiple rights violations. On November 20th, the day before the planned protest, millions of Claro, Movistar, and Tigo users reportedly received a mass text message from the government

encouraging a peaceful demonstration; the message could also be understood, though, as a disincentive to participate. <sup>81</sup>

Colombian social movements increasingly use online platforms for advocacy. Campaigns such as #CompartirNoEsDelito (Sharing is not a crime) have sought to promote open access to information and protest Colombia's intellectual property law, which can carry harsh penalties and has been used to punish academics who shared research online. <sup>82</sup>

## C. Violations of User Rights

*During the coverage period, a journalist served a 10-day prison sentence for refusing to remove articles from his news site and personal website. Two investigations revealed that the military used both open-source and more sophisticated surveillance technology and monitored at least 130 people, including 30 journalists. Amid a legal environment that obliges service providers to collaborate with intelligence agencies and retain subscriber data for five years, the government authorized mobile providers to share users' personal data with public authorities responding to the COVID-19 pandemic. Several cyberattacks targeted news sites that reported on sensitive topics.*

**C1** 0-6 pts

**Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?**

**3/6**

Article 20 of the constitution guarantees freedom of information and expression and prohibits prior restraint. Article 73 further provides for the protection of “the liberty and professional independence” of “journalistic activity.” Although there are no specific provisions protecting freedom of expression online, bloggers have the same liberties and protections as print or broadcast journalists. <sup>83</sup> The Constitutional Court confirmed the application of such protections to the internet in a 2012 <sup>84</sup> g.

**84**

**TOP**

Impunity for perpetrators of violence is a pervasive problem in Colombia's judicial system and represents a grave threat to freedom of expression, according to rights advocates. <sup>85</sup>

**Are there laws that assign criminal penalties or civil liability for online activities?**

**2/4**

Colombia maintains criminal penalties for defamation. According to the Colombian penal code, individuals accused of insult can face up to six years in jail and a fine, while individuals accused of libel can face between fifteen months and four-and-a-half years in jail, also with possible fines. <sup>86</sup> Cases pertaining to online defamation have occasionally been brought before the court with varying outcomes.

The penal code includes a concerning provision regarding online publication or reproduction of insults. According to Article 222, “whoever publishes, reproduces, or repeats insult or libel” may also be subject to punishment. This article raises concerns as it leaves open the possibility for charges of indirect insult and libel. The penal code also establishes the use of “social mediums of communication or of other collective divulgence” as an aggravating circumstance that can increase the penalty for insult or libel. <sup>87</sup> However, courts have not held intermediaries responsible for defamatory content created or shared by third parties.

Between 2018 and 2019, two bills, PL 60/18 (on strengthening citizens’ security) and PL 74/18 (on combatting cybercrimes), which would establish worrisome restrictions for online expression, were presented and debated. The bills, which were later combined, aimed to prohibit the nonconsensual dissemination of sexual content. However, the proposal was criticized for being overly broad; it originally focused on “intimate” content, and makes no exceptions for other content that can be considered “sexual.”

<sup>88</sup> The legislation was not yet approved as of June 2020.

Another bill proposed in 2019 would restrict online expression. PL 176/19, which aims to regulate social networks, seeks to prohibit citizens from publishing any type of data, information, files, photographs, or videos of another person without their express written consent, while prohibiting the creation of profiles “that do not represent a real person.” It would apply, for example, to accounts for pets or for parody. It also seeks to prohibit the publication of insults, prohibit people from “overexposing” their own privacy, oblige them to be “discreet” in their publications, and prohibit users from disclosing “sensitive” personal information, such as financial information, contact details, or “sentimental information.” In addition, users would be prohibited

from accessing “inappropriate content,” though how that content would be defined is not clear. <sup>89</sup>

Colombia has harsh penalties for copyright violations and lacks flexible fair use standards employed in many countries. In a prominent case, in 2014, student Diego Gómez was charged with violating copyright violations for uploading an academic thesis onto Scribd. <sup>90</sup> Digital rights groups heavily criticized the decision to prosecute, especially when he did not claim to have authored the thesis and did not profit by sharing it. <sup>91</sup> He was finally cleared of criminal charges in 2017. <sup>92</sup>

**C3** 0-6 pts

**Are individuals penalized for online activities?**

**5/6**

Prosecution, imprisonment, or detention for ICT activities is quite rare in Colombia, and writers, commentators, and bloggers are not systematically subject to imprisonment or fines for posting material on the internet.

However, in March 2020, journalist Edison Lucio Torres served a 10-day prison sentence in the Los Caracoles police station after being sentenced by a criminal court in the city of Cartagena; the court also handed down a \$2,600 fine. <sup>93</sup> The decision came after Torres did not comply with an order to remove articles from his news site Vox Populi, as well as his personal website. The articles centered on 2016 reports about a religious leader who allegedly used church donations for personal expenses; the subject and his wife subsequently filed a complaint in November 2019, resulting in the removal order. <sup>94</sup> The judicial process was criticized for numerous flaws. <sup>95</sup>

The case demonstrates a small but persistent trend in which, as the public debate is being adjudicated, imprisonment is demanded as a form of rectification. Similarly, in August 2018, Juvenal Bolívar, a journalist at news outlet *Corillos*, and Sofía Ortiz Delgado, a former staff member there, served a 10-day sentence that was arbitrarily imposed by a civil court in the city of Bucaramanga. The sentence was issued after Bolívar refused to comply with a ruling ordering him to withdraw an investigation into a city official from his website, after a process plagued by procedural irregularities. <sup>96</sup>

In June 2020, after the coverage period, three contributors to *ab zurdo*, a photography account on Instagram, were detained in Medellín while covering a



demonstration against the government's COVID-19 response. They were fined for violating the city's lockdown. **97**

**C4** 0-4 pts

**Does the government place restrictions on anonymous communication or encryption?**

**3/4**

Colombia has no general restrictions against anonymous communication, and there are no registration requirements for bloggers or cybercafé owners, though users must register to obtain telecommunication services. Police have access to a database that must be maintained by telecommunication service providers. This database contains user data, such as name, identification number, place and residence address, mobile phone number, and service activation date. **98** Users must provide accurate information under penalty of perjury, which is punishable by a minimum of six years in prison. **99**

In April 2017, the prosecutor general announced a proposal to force WhatsApp and other internet intermediaries to decrypt users' communications for law enforcement purposes. **100** Even though the proposal was never enacted, the announcement raised concerns about the state's surveillance ambitions, as well as officials' lack of understanding regarding technology like encryption. **101** (Providers that encrypt communications end-to-end cannot decrypt them.)

Since 1993, Colombian law has banned the use of "communication devices that use the electromagnetic spectrum" to send "encrypted messages or messages in unintelligible language." **102** In response to an information request, the ICT ministry explained that those provisions apply only "to the content of the communications, not the encryption of the medium." Despite the ambiguous wording of the law, the ICT ministry further claimed that these provisions only apply to radio-like devices and not to the internet. **103** The Intelligence and Counterintelligence Act stipulates that telecommunications service providers may only offer encrypted voice service intelligence agencies and "high government" officials. **104**

**TOP**

**C5** 0-6 pts

**Does state surveillance of internet activities infringe on users' right to privacy?**

**2/6**

---

Intercepting personal communications in Colombia is authorized only for criminal investigation purposes and legally requires a judicial order. <sup>105</sup> Colombian law allows intelligence agencies to monitor devices that use the electromagnetic spectrum to transmit wireless communication without a judicial order. <sup>106</sup>

Episodes of extralegal surveillance carried out by intelligence agencies, the army, and the police have constituted an ongoing scandal in Colombia in recent years. Some steps have been taken to punish perpetrators of illegal surveillance, although it seems unlikely that these efforts have changed the overall environment, as intelligence agencies continue to operate with minimal oversight. Concerns about illegal surveillance by certain sectors of the government and military persist. Several Colombian civil society organizations have criticized the excessive and apparently uncontrolled use of surveillance tools in the country, which they argue has been facilitated by “weak legislation” on intelligence matters. <sup>107</sup>

In January 2020, the magazine *Semana* published an investigation revealing the military’s use of open-source intelligence and sophisticated equipment. During 2019, technology provided by the United States to address drug trafficking and the fight against guerrillas was used to spy on politicians, magistrates, generals, social leaders, activists, and journalists. According to IFEX, files on each target included “excerpts of their conversations on social media and messaging apps, photographs, videos, network of contacts, and maps tracing their movements.” Most of the information was obtained through open source. However, other technology, including International Mobile Subscriber Identity (IMSI) catcher equipment and a malware system called Invisible Man was also employed, as was the artificial intelligence tool Voyager, which was created by an Israeli company. <sup>108</sup>

*Semana* published the results of another investigation in May 2020, which noted that 130 people were targeted for surveillance, including 30 journalists from outlets including the *New York Times*, *Wall Street Journal*, *Semana*, and *La Liga Contra el Silencio*. The regional head of Human Rights Watch (HRW) was also surveilled. <sup>109</sup> The *New York Times* identified journalist Nicholas Casey, who reported on Major General Nicacio Martínez Espinel’s orders to increase the number of killed militants and criminals in May 2019, as a surveillance target. <sup>110</sup> (Major General Martínez was

relieved of his post that December.) Also targeted were social leaders and human rights defenders from the Inter-Ecclesial Commission for Justice and Peace. **111**

Ahead of the May 2020 report's publication, at least 11 army officials were fired and one resigned. **112** While the military carried out an investigation, **113** the general prosecutor's office opened its own, though no progress on that effort was publicized at the end of the coverage period. **114**

Data sharing, including through apps, has been initiated as part of Colombia's COVID-19 pandemic response (see C6), but concerns have been raised about the privacy rights of users and the effectiveness of the apps. Privacy International warned that the government's COVID-19 app, Coronapp, will not function without the user providing information including their name, sex, ethnicity, and email address, and provides no clarity on how that data will be used or protected. Coronapp notably asks users if they participated in mass protests within the last eight days. **115**

In 2015, documents leaked from the technology company Hacking Team, which is known to provide spyware to governments, suggested that the Colombian government had contracts with the company. Leaked emails referenced the National Police Office's (OPN) purchase of Hacking Team's Remote Control System (RCS) product, Galileo, which is capable of accessing and hijacking target devices' keyboards, microphones, and cameras. Police would only acknowledge having contractual ties with a Colombian company called Robotec, which distributes Hacking Team's services, **116** though the leaked documents indicate that the national police contacted Hacking Team directly to activate spyware. **117** Another leaked email suggested that the US Drug Enforcement Agency (DEA) may be conducting surveillance in Colombia. **118**

That same year, police reportedly said that they would start testing a centralized platform for monitoring and analysis known as PUMA. They said telephone lines would be subject to monitoring, but not social networks and chats. **119** The prosecutor general's office previously ordered police to stop developing PUMA because of a lack of transparency and insufficient guarantees to ensure its lawful use. Journalists' <sup>TOP</sup> reported that the government was investing over \$100 million in a monitoring platform in 2013. The system was intended to provide the government with the capacity to intercept telephone and internet communications, including private messages, in real time. **120**

Also in 2015, Privacy International found that the Bogotá police bought technology from the companies NICE (sold to Elbit Systems the same year) and Verint that could intercept phone calls in order to monitor government opponents. According to a 2018 investigation by Israeli newspaper *Haaretz*, Colombia has continued to purchase technology from Verint. <sup>121</sup>

Courts have sought to rein in illegal surveillance, sentencing former public officials involved in wiretapping scandals. In September 2018, the general attorney's office filed criminal charges against a former high-ranking police official, retired general Humberto Guatibonza, along with a hacker and three former army members for alleged illicit association, abusive access to an IT system, personal data violation, malicious software use, and illegal interceptions. The individuals were placed under house arrest. <sup>122</sup> The investigation was still ongoing at the end of the coverage period.

Several former heads of the now-dismantled government Administrative Security Department (DAS), notably Fernando Tabares, Jorge Noguera, and María del Pilar Hurtado, were convicted for illegal wiretapping in 2015. Bernardo Moreno, former secretary of the president's office, also received an eight-year prison sentence on charges of illegally intercepting private communications of journalists, politicians, and civil society groups. <sup>123</sup> Noguera was called to trial again, and was sentenced to 94 months in prison in 2017 for his part in illegal interception activities against human rights defenders, journalists, and civil society organizations. <sup>124</sup> Military officials were fired in early 2015 following a high-profile wiretapping scandal. <sup>125</sup>

**C6** 0-6 pts

**Are service providers and other technology companies required to aid the government in monitoring the communications of their users?**

**3/6**

*Score Change: The score declined from 4 to 3 because the government authorized mobile providers to share users' personal data with public authorities as part of its COVID-19 response, amid a legal environment that obliges service providers to collaborate with intelligence agencies and retain subscriber data for five years.*

**TOP**

While some constitutional and legal protections regulate the government's use of data, service providers in Colombia are obligated to share data with the intelligence

community with limited judicial review; providers are also obligated to capture and store user data for use in criminal investigations.

Service providers are required to collaborate with intelligence agencies by providing access, when feasible, to the communications history, location data, or technical data of any specific user without a warrant; intelligence agencies conducting an authorized operation only need to request the data. However, Colombian intelligence and counterintelligence agencies are also subject to Statutory Law 1621 of 2013, which binds agencies to respect “rights to honor, good name, personal and family privacy, and due process.” Article 4 restricts the discriminatory use of intelligence data, including on the basis of gender, race, or origin (see C5). <sup>126</sup>

Service providers are also obliged to retain subscriber data for the purposes of criminal investigations and intelligence activities for a period of five years. <sup>127</sup> An additional threat to user privacy comes in the form of Article 2 of Decree 1704 (2012), which requires that ISPs create access points that capture communications traffic on their networks for criminal investigation purposes—which can be used under the prosecutor general’s authorization. A service provider that does not comply with these obligations faces fines and could lose its operating license. <sup>128</sup>

In March 2020, the Superintendence of Industry and Commerce (SIC), a consumer protection agency that operates under the purview of Colombia’s trade ministry, released a circular that authorized telecommunications firms to share user data with public authorities as part of the country’s COVID-19 response. While public entities are obliged to secure data and respect its confidentiality, <sup>129</sup> the decision opens users to risks including discrimination, undue surveillance, invasion of privacy, and the revelation of journalistic sources. The circular does not specify what data should be collected and imposes no time limit. <sup>130</sup>

## C7 0-5 pts

|                                                                                                                                                                    |          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| <b>Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?</b> | <b>5</b> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|

**TOP**

Corruption, longstanding armed conflict and associated surveillance, and the war against drugs are the greatest threats to freedom of expression in Colombia, although online journalists have not been attacked as often as print journalists. According to



FLIP, at least 22 journalists have been murdered and many more have been threatened since 2005. <sup>131</sup> There is no broad trend of retaliation specifically for online content, but the high level of intimidation towards media and human rights defenders creates a climate of fear that also affects online journalists.

In April 2020, Eder Narváez Sierra, the creator and editor of news site NP Noticias and a television correspondent, received death threats over WhatsApp from an individual claiming to lead the Los Caparrapos armed group, which is linked to drug trafficking. Narváez speculated that an article he wrote covering two homicides, which also identified the victims, may have brought the threat about. The individual who wrote to Narváez claimed that they were responsible for the murders. <sup>132</sup>

During the coverage period, FLIP observed a number of cases demonstrating a continued trend of extralegal intimidation against online journalists as a consequence of their work. For example, in August 2019, journalist Vicky Dávila received several tweets threatening both her and her family after a discussion on Twitter with Senator Gustavo Petro. The conversation was spurred by Dávila's sharing of a video that showed Magdalena gubernatorial candidate Carlos Caicedo, a Petro ally, being attacked by eggs. <sup>133</sup> During the previous month, journalist Gabriel Angarita, of the digital television channel Tvcucuta, reported receiving a death threat through WhatsApp and another threat on Facebook. <sup>134</sup>

Also during the coverage period, Bogotá-based CNN correspondent Asdrúbal García was threatened on Facebook after he denounced another threat made against documentary filmmaker Jonathan Palacios on his profile. Palacios was investigating irregularities in the administration of the mayor of the municipality of Anolaima. Asdrúbal received a message from a person identified as "José Medina," who told him to "shut his mouth so flies would not enter." <sup>135</sup>

#### **C8** 0-3 pts

**Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?**

- / 3  
**TOP**

In 2019 and 2020, FLIP recorded at least 18 cyberattacks against websites. <sup>136</sup>



In early March 2020, online news outlet La Oreja Roja (the Red Ear) published an article discussing late drug trafficker José Guillermo “Añe” Hernández’s suspected involvement in a vote-buying campaign during the 2018 presidential election. The website was made inaccessible the weekend after the article was published. **137**

In November 2019, the website of newsmagazine *Cartel Urbano* was attacked, and was inaccessible for several hours. The technical attack took place after the outlet published a note denouncing a police search of their office. The newsmagazine’s social media accounts were also hacked, and social media comments were posted by outside individuals. **138**

Also in November 2019, the website of CeroSetenta, a digital media initiative sponsored by the University of the Andes, suffered a distributed denial-of-service (DDoS) attack. The attack came after the outlet reported that the police attempted to restrict an article from another outlet, which informed readers how to protect themselves while participating in protests. **139**

According to an editor of newsmagazine *Don Jumento*, the outlet has been unable to administer its own website since February 2020 due to an apparent password change initiated by someone other than a staff member. Meanwhile, Mario Cepeda, the director of digital news site Página10, informed FLIP that he could no longer administer the outlet’s Facebook page in September 2019. A systems engineer found that Cepeda’s inability to manage the site was the result of a hack, apparently performed by an expert. While the page remained online, Cepeda was unable to share content to it.

## Footnotes

- 1** Ministry of Information and Communications Technologies of the Republic of Colombia, “Boletín Trimestral de las TIC – Cifras Cuarto Trimestre de 2019 [ICT Quarterly Bulletin – Figures of the Fourth Quarter of 2019],” April 2020, [https://colombiatic.mintic.gov.co/679/articles-135691\\_archivo\\_pdf.pdf](https://colombiatic.mintic.gov.co/679/articles-135691_archivo_pdf.pdf).
- 2** Consultant calculation due the change of measure unit, from internet penetration (2018) to the number of connections per every 100 inhabitants (2019). **TOP**
- 3** Ministry of Information and Communications Technologies of the Republic of Colombia, “Planes pilotos y entregar conectividad a 20 millones de colombianos es la meta del MinTic

[Pilot plans and deliver connectivity to 20 million Colombians is the goal of the MinTic],” January 24, 2019, [https://www.mintic.gov.co/porta/604/w3-article-82248.html?\\_noredirect=1](https://www.mintic.gov.co/porta/604/w3-article-82248.html?_noredirect=1).

- 4 “Colombia – April 2020,” Ookla® Speedtest, June 14, 2020, <https://web.archive.org/web/20200614214251/https://www.speedtest.net/gl...>
- 5 Diego Ojeda, “Cambia la definición de banda ancha, ¿Colombia está preparada? [The definition of broadband has changed, is Colombia ready?],” El Espectador, January 4, 2019, <https://www.elespectador.com/tecnologia/cambia-la-definicion-de-banda-a...>

More footnotes



#### On Colombia

See all data, scores & information on this country or territory.

See More >

#### Country Facts

Global Freedom Score

**65/100** Partly Free

Internet Freedom Score

**66/100** Partly Free

Freedom in the World Status

**Partly Free**

Networks Restricted

**No**

Social Media Blocked

**No**

Websites Blocked

**No**

Pro-government Commentators

**No**

TOP

Users Arrested

**Yes**

*In Other Reports*

Freedom in the World 2020

*Other Years*

2019

## Be the first to know what's happening.

Join the Freedom House monthly newsletter

Email

Subscribe

### ADDRESS

1850 M St. NW Floor 11  
Washington, DC 20036  
(202) 296-5101

### GENERAL INQUIRIES

[info@freedomhouse.org](mailto:info@freedomhouse.org)

### PRESS & MEDIA

[press@freedomhouse.org](mailto:press@freedomhouse.org)

@2021 FreedomHouse

**TOP**